UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/690,083	10/16/2000	Craig L. Ogg	40630/RRT/S850	2004

23363 7590 01/06/2005

CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
BACKER, FIRMIN	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 01/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/690,083	OGG ET AL.	
	Examiner	Art Unit	
	Firmin Backer	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 October 2004* .

2a)☒ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-120* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-120* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

Response to Amendment

This is in response to an amendment file on October 29th, 2004. In the amendment, claims 1 and 42 have been amended, no claim has been canceled, and no claim has been added. Claims 1-120 remain pending in the letter.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-120 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leon (U.S. Patent No 6,424,954) in view Cordery et al (U.S. Patent No. 6,567,794).

3. As per claim 1, Leon teaches a cryptographic device (*SMD, 110a, 110b comprise a cryptographic module)* for securing data on a computer network *(network 100a, 100b, fig 1A, 1B)* comprising a processor (*processor, 210)* programmed to authenticate (*authenticate)* a plurality of users (*users, 120, fig 1A, 1B)* on the computer network *(network 100a, 100b, fig 1A, 1B)* for secure processing of a value bearing item (*postal indicium, fig 9)* wherein the processor include a state machine for determine a state corresponding to availability of one or more commands *(see abstract, figs 5a –7, column 9 line 35-67)*, a cryptographic engine (*cryptographic*

module) for cryptographically protecting data, and an interface (*interface, 222, 236, fig 2A)* for communicating with the computer network (*see column 4 line 21-55).* Leon fails to teach a memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users and a the cryptographic module is remotely located from the user wherein once the user is authenticated, the cryptographic device enters an operational state in which it continues to authenticate the user with respect to one or more transactions requested by the user. However, Cordery et al teaches a memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users (*see abstract, fig 1, 4, 5, column 4 line 23-49)* and a cryptographic module is remotely located from the user and and wherein once the user is authenticated, the cryptographic device enters an operational state in which it continues to authenticate the user with respect to one or more transactions requested by the user (*see figs 1, 3 and 5, column 1 lines 24-65).* Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Leon's inventive concept to include Cordery et al's memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users and a the cryptographic module is remotely located from the user and wherein once the user is authenticated, the cryptographic device enters an operational state in which it continues to authenticate the user with respect to one or more transactions requested by the user because this would have protected the privacy of those transaction and the privacy of the user thereby making easier for the system to retrieve and identify the user of the system thereby eliminated stolen and relocated meter problems and simplifies meter management in general.

4. As per claims 2-8, Leon teaches a cryptographic device wherein the state machine includes one or more of an uninitialized state, an initialized state, an operational state, an administrative state, an exporting shares state, an importing shares state, and an error state *(see abstract, figs 5a –7, column 9 line 59-67)*.

5. As per claim 9, Leon teaches a cryptographic device wherein on or more command corresponding to the uninitialized state includes a command for start initializing *(figs 6a-6e, column 10 lines 10-16)*.

6. As per claim 10, Leon teaches a cryptographic device wherein the one or more commands corresponding to the initialized state includes commands for one or more of get status command, initialize access control database command, logon command, logoff command, query current user role command, query current user ID command, session management commands, audit entry creation command, generate master key set command, and generate transport key pair commands *(see abstract, figs 5a –7, column 10 lines 10-16, 13 lines 26-47)*.

7. As per claim 11, Leon teaches a cryptographic device wherein the one or more commands corresponding to the operational state include commands for one or more of access control, session management, key management, and audit support *(see column 11 lines 36-43)*.

8. As per claim 12, Leon teaches a cryptographic device wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command, view access control database command, change password command, set clock command, and set Status command (*see fig 5b, column 13 lines 63-14 line 31)*.

9. As per claim 13, Leon teaches the inventive concept as disclosed in claims 1 and 11. Leon fail to teach a cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command. However, Cordery et al teaches a cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command (*see abstract, fig 1, 4, 5, column 4 line 23-49)*. Therefore, it would have been obvious to one of ordinary skill in that art at the time the invention was made to modify Leon's inventive concept to include Cordery et al's cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command because this would have avoided the need for key encryption in the user's computer.

10. As per claim 14, Leon teaches a cryptographic device wherein the commands for key management include one or more of export transport public key command, start importing MKS command, create MKS shares command, generate MKS command, activate MKS command, delete dormant MKS command, global decrypt and MAC command, compute MAC command, verify MAC, and encryption and MAC translation commands (*see column 13 lines 36-62).*

11. As per claim 15, Leon teaches a cryptographic device wherein the commands for audit support include one or more of create audit entry command, create audit key command, and export audit verification key command (*see abstract, figs 5f, see column 18 line 18-40, 24 line 60-25 line 5).*

12. As per claim 16, Leon teaches a cryptographic device wherein the one or more commands corresponding to the administrative state include commands for one or more of create account command, delete account command, modify account command, view access control database command, end admin command, logon command, logoff command, query current user role command, query current user ID command, set clock command, get status command, session management commands, and audit entry creation command (*see abstract, figs 5a –7, see column 9 line 35-67).*

13. As per claim 17, Leon teaches a cryptographic device wherein the one or more commands corresponding to the exporting shares state include commands for one or more of logon command, logoff command, query Current User Role command, query current user ID

command, export share command, abort export command, get status command, session management commands, and audit entry creation command (*see column 8 line 63-9 line 19)*.

14. As per claim 18, Leon teaches a cryptographic device wherein the one or more commands corresponding to the importing shares state include command for one more of logon command, logoff command, query current user role command, query current user ID command, export transport public key command, import share command, combine shares command, set status command, session management commands, and audit entry creation command (*see column 8 line 63-9 line 19)*.

15. As per claim 19, Leon teaches a cryptographic device wherein the one or more commands corresponding to the error state include commands for one or more of get status command, and access control queries command (*see column 10 lines 39-46)*.

16. As per claim 20, Leon teaches a cryptographic device further comprising computer executable code to keep track of a present operational state *(see abstract, figs 5a –7, see column 9 line 35-67)*.

17. As per claim 21, Leon teaches a cryptographic device wherein the processor is programmed to verify that the authenticated user is authorized to assume a role and perform a corresponding operation (*see fig 5A, column 12 lines 30-42, table 1 in column 12)*.

18. As per claim 22, Leon teaches a cryptographic device wherein the cryptographic device includes a computer executable code for preventing unauthorized disclosure of data (*see fig 5E-5E-2, column 17 lines 47-54, 19 lines 33-42).*

19. As per claim 23, Leon teaches a cryptographic device wherein the cryptographic device includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user (*see fig 1A, 1B).*

20. As per claims 24-27, Leon teaches a cryptographic device wherein the value bearing item include a postage value including a postal indicium comprises a digital signature, a postage amount, an ascending register of used postage and descending register of available postage (*see fig 8F, table 3 column 42).*

21. As per claim 28-33, Leon teaches a cryptographic device wherein the value bearing item is a ticket, a bar code, a coupon, a currency, a traveler's check, a voucher (*see fig 9).*

22. As per claim 34, Leon teaches a cryptographic device wherein each security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, data and time of last transaction, last challenge received from a respective client subsystem, an operational

state of the respective device, expiration dates for keys, and a passphrase repetition list (*see fig 8F, table 3 column 42)*.

23. As per claim 35, Leon teaches a cryptographic device wherein each security device transaction data includes information to define the present operational state of the device *(see abstract, figs 5a –7, see column 9 line 35-67)*

24. As per claim 36, Leon teaches a cryptographic device wherein the processor is capable of sharing a secret with a plurality of other cryptographic devices (*see column 13 lines 48-62)*.

25. As per claim 37-40, Leon teaches a cryptographic device wherein the processor and the cryptographic engine generate a master key set (MKS) including a Master Encryption Key (MEK) used to encrypt keys when stored outside the device and a Master Authentication Key (MAK) used to compute a DES MAC for signing keys when stored outside of the device exported to other cryptographic devices by any cryptographic device and wherein the cryptographic engine is programmed to perform one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms (*see column 13 lines 48-62)*.

26. As per claim 41, Leon teaches a cryptographic device wherein at least one of the plurality of users is an enterprise account (*see fig 1)*.

27. As per claims 42 and 44, Leon teaches a method for securing (*SMD, 110a, 110b comprise a cryptographic module)* data (*postal/metering information)* on a computer network *(network 100a, 100b, fig 1A, 1B)* including a plurality of users (*users, 120, fig 1A, 1B)* comprising authenticating (*authenticate)* and authorizing (*authorizing)* the plurality of users (*users, 120, fig 1A, 1B)* for secure processing of a value bearing item (*postal indicium, fig 9)* and determining a state machine for availability of one or more commands *(see abstract, figs 5a –7, column 9 line 35-67)*. Leon fails to teach a memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users and a the cryptographic module is remotely located from the user and wherein once the user is authenticated, the cryptographic device enters an operational state in which it continues to authenticate the user with respect to one or more transactions requested by the user. However, Cordery et al teaches a memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users (*see abstract, fig 1, 4, 5, column 4 line 23-49)* and a cryptographic module is remotely located from the user and wherein once the user is authenticated, the cryptographic device enters an operational state in which it continues to authenticate the user with respect to one or more transactions requested by the user (*see figs 1, 3 and 5, column 1 lines 24-65).* Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Leon's inventive concept to include Cordery et al's memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users and a the cryptographic module is remotely located from the user and the cryptographic device enters

an operational state in which it continues to authenticate the user with respect to one or more transactions requested by the user because this would have protected the privacy of those transaction and the privacy of the user thereby making easier for the system to retrieve and identify the user of the system thereby eliminated stolen and relocated meter problems and simplifies meter management in general.

28. As per claim 43, Leon teaches a method for securing of printing the value bearing item *(see fig 9)*.

29. As per claim 45, Leon teaches a method for securing of loading a security device transaction data related to the cryptographic device when the user requests to operate on a value bearing item (*see column 9 lines 1-10)*.

30. As per claim 46, Leon teaches a method for securing of authenticating the identity of each user and verifying that the identified user is authorized to assume a role and to perform a corresponding operation (*see column 8 line 45-61)*.

31. As per claims 47-53, Leon teaches a method wherein the state machine includes one or more of an uninitialized state, an initialized state, an operational state, an administrative state, an exporting shares state, an importing shares state, and an error state *(see abstract, figs 5a –7, see column 9 line 35-67)*.

32. As per claim 54, Leon teaches a method wherein on or more command corresponding to the uninitialized state includes a command for start initializing (*see figs 5A, 5B, 6).*

33. As per claim 55, Leon teaches a method wherein the one or more commands corresponding to the initialized state includes commands for one or more of get status command, initialize access control database command, logon command, logoff command, query current user role command, query current user ID command, session management commands, audit entry creation command, generate master key set command, and generate transport key pair commands (*see fig 5A, 5B, column 10 line 10-16).*

34. As per claim 56, Leon teaches a method wherein the one or more commands corresponding to the operational state include commands for one or more of access control, session management, key management, and audit support (*see abstract, figs 5f, see column 18 line 18-40, 24 line 60-25 line 5).*

35. As per claim 57, Leon teaches a method wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command, view access control database command, change password command, set clock command, and set Status command (*see column 8 line 45-62).*

36. As per claim 58, Leon teaches the inventive concept as disclosed in claims 1 and 11. Leon fails to teach a cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command. However, Cordery et al teaches a cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command (*see abstract, fig 1, 4, 5, column 4 line 23-49).* Therefore, it would have been obvious to one of ordinary skill in that art at the time the invention was made to modify Leon's inventive concept to include Cordery et al's cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command because this would have avoided the need for key encryption in the user's computer.

37. As per claim 59, Leon teaches a method wherein the commands for key management include one or more of export transport public key command, start importing MKS command, create MKS shares command, generate MKS command, activate MKS command, delete dormant MKS command, global decrypt and MAC command, compute MAC command, verify MAC, and encryption and MAC translation commands (*see fig 5E-5E-2, column 17 lines 47-54, 19 lines 33-42).*

38. As per claim 60, Leon teaches a method wherein the commands for audit support include one or more of create audit entry command, create audit key command, and export audit verification key command (*see abstract, figs 5f, see column 18 line 18-40, 24 line 60-25 line 5).*

39. As per claim 61, Leon teaches a method wherein the one or more commands corresponding to the administrative state include commands for one or more of create account command, delete account command, modify account command, view access control database command, end admin. command, logon command, logoff command, query current user role command, query current user ID command, set clock command, get status command, session management commands, and audit entry creation command (*see column 8 lines 63-9 line 33).*

40. As per claim 62, Leon teaches a method wherein the one or more commands corresponding to the exporting shares state include commands for one or more of logon command, logoff command, query Current User Role command, query current user ID command, export share command, abort export command, get status command, session management commands, and audit entry creation command (*see fig 5A, column 12 lines 30-42, table 1 in column 12).*

41. As per claim 63, Leon teaches a method wherein the one or more commands corresponding to the importing shares state include command for one more of logon command, logoff command, query current user role command, query current user ID command, export transport public key command, import share command, combine shares command, set status

command, session management commands, and audit entry creation command (*see fig 5A, column 12 lines 30-42, table 1 in column 12)*.

42. As per claim 64, Leon teaches a method wherein the one or more commands corresponding to the error state include commands for one or more of get status command, and access control queries command (*see column 10 lines 39-46)*.

43. As per claims 65-68, Leon teaches a method of printing a postage value including a postal indicium comprises a digital signature, a postage amount, an ascending register of used postage and descending register of available postage (*see fig 8F, table 3 column 42)*.

44. As per claim 69-71, Leon teaches a method or printing a ticket, a bar code, a coupon, (*see fig 9)*.

45. As per claim 72, Leon teaches a security system (*SMD, 110a, 110b comprise a cryptographic module)* for securing data (*postal/metering information)* in a computer network *(network 100a, 100b, fig 1A, 1B)* comprising a plurality of user terminals (*users, 120, fig 1A, 1B)* coupled (*connected)* to the computer network *(network 100a, 100b, fig 1A, 1B)*, a cryptographic device (*cryptographic key)* remote from the plurality of user terminals and coupled to the computer network, wherein the cryptographic device (*SMD, 110a, 110b comprise a cryptographic module)* includes a state machine (*state diagram/method, fig 6A)* for determining a state machine for availability of one or more commands available to authenticating user. Leon

fails to teach a plurality of security device transaction data for ensuring authenticity of the one or more users, wherein each security device transaction data is related to a user and of managing value of available to user. However, Cordery et al teaches a plurality of security device transaction data for ensuring authenticity of the one or more users, wherein each security device transaction data is related to a user (*see abstract, fig 1, 4, 5, column 4 line 23-49)* and of managing value of available to user (*see figs 1, 3 and 5, column 1 lines 24-65)*. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Leon's inventive concept to include Cordery et al's a plurality of security device transaction data for ensuring authenticity of the one or more users, wherein each security device transaction data is related to a user and of managing value of available to user because this would have protected the privacy of those transaction and the privacy of the user thereby making easier for the system to retrieve and identify the user of the system thereby eliminates stolen and relocated meter problems and simplifies meter management in general.

46. As per claim 73, Leon teaches a security system wherein the security device transaction data related to a user is loaded into the cryptographic device when the user requests to operate on a value bearing item (*see fig 9)*.

47. As per claims 74-80, Leon teaches a method wherein the state machine includes one or more of an uninitialized state, an initialized state, an operational state, an administrative state, an exporting shares state, an importing shares state, and an error state *(see abstract, figs 5a –7, see column 9 line 35-67)*.

48. As per claim 81, Leon teaches a method wherein on or more command corresponding to the uninitialized state includes a command for start initializing (*see figs 5A, 5B, 6)*.

49. As per claim 82, Leon teaches a method wherein the one or more commands corresponding to the initialized state includes commands for one or more of get status command, initialize access control database command, logon command, logoff command, query current user role command, query current user ID command, session management commands, audit entry creation command, generate master key set command, and generate transport key pair commands (*see fig 5A, 5B, column 10 line 10-16)*.

50. As per claim 83, Leon teaches a method wherein the one or more commands corresponding to the operational state include commands for one or more of access control, session management, key management, and audit support (*see abstract, figs 5f, see column 18 line 18-40, 24 line 60-25 line 5)*.

51. As per claim 84, Leon teaches a method wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command, view access control database command, change password command, set clock command, and set Status command (*see column 8 line 45-62)*.

52. As per claim 85, Leon teaches the inventive concept as disclosed in claims 1 and 11. Leon fails to teach a cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command. However, Cordery et al teaches a cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command (*see abstract, fig 1, 4, 5, column 4 line 23-49).* Therefore, it would have been obvious to one of ordinary skill in that art at the time the invention was made to modify Leon's inventive concept to include Cordery et al's cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command because this would have avoided the need for key encryption in the user's computer.

53. As per claim 86, Leon teaches a method wherein the commands for key management include one or more of export transport public key command, start importing MKS command, create MKS shares command, generate MKS command, activate MKS command, delete dormant MKS command, global decrypt and MAC command, compute MAC command, verify MAC, and encryption and MAC translation commands (*see fig 5E-5E-2, column 17 lines 47-54, 19 lines 33-42).*

54. As per claim 87, Leon teaches a method wherein the commands for audit support include one or more of create audit entry command, create audit key command, and export audit verification key command (*see column 8 line 45-62).*

55. As per claim 88, Leon teaches a method wherein the one or more commands corresponding to the administrative state include commands for one or more of create account command, delete account command, modify account command, view access control database command, end admin command, logon command, logoff command, query current user role command, query current user ID command, set clock command, get status command, session management commands, and audit entry creation command (*see fig 5E-5E-2, column 17 lines 47-54, 19 lines 33-42).*

56. As per claim 89, Leon teaches a method wherein the one or more commands corresponding to the exporting shares state include commands for one or more of logon command, logoff command, query Current User Role command, query current user ID command, export share command, abort export command, get status command, session management commands, and audit entry creation command (*see fig 5A, column 12 lines 30-42, table 1 in column 12).*

57. As per claim 90, Leon teaches a method wherein the one or more commands corresponding to the importing shares state include command for one more of logon command, logoff command, query current user role command, query current user ID command, export

transport public key command, import share command, combine shares command, set status command, session management commands, and audit entry creation command (*see fig 5E-5E-2, column 17 lines 47-54, 19 lines 33-42).*

58. As per claim 91, Leon teaches a method wherein the one or more commands corresponding to the error state include commands for one or more of get status command, and access control queries command (*see abstract, figs 5f, see column 18 line 18-40, 24 line 60-25 line 5).*

59. As per claim 92, Leon teaches a security system comprising computer executable code to keep track of a present operational state (*see column 8 line 45-62).*

60. As per claim 93, Leon teaches a security system wherein the processor is programmed to verify that the authenticated user is authorized to assume a role and perform a corresponding operation (*see column 8 line 45-62).*

61. As per claim 94, Leon teaches a security system wherein the system includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user (*see fig 1A, 1B).*

62. As per claims 95-98, Leon teaches a secured system wherein a postage value including a postal indicium comprises a digital signature, a postage amount, an ascending register of used postage and descending register of available postage (*see fig 8F, table 3 column 42).*

63. As per claim 99-100, Leon teaches a security system wherein the value bearing item include a bar code is a ticket (*see fig 9).*

64. As per claim 101, Leon teaches a security system wherein each security device transaction data includes information to define the present operational state of the device (*see fig 6A, column 9 line 35-67).*

65. As per claim 102, Leon teaches a security system wherein the cryptographic engine is programmed to perform one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms (*see column 11 lines 51-12 line 4, 13 line 47-62).*

66. As per claim 103, Leon teaches a method or printing a ticket, a bar code, a coupon, (*see fig 9).*

67. As per claim 104, Leon teaches a method for securing data (*SMD, 110a, 110b comprise a cryptographic module)* in a computer network *(network 100a, 100b, fig 1A, 1B)* having a plurality of user terminals (*users, 120, fig 1A, 1B)* the method comprising and verifying that a

user is authorized to assume a role and determining a state in a state machine for availability of one or more commands (*see fig 1A, 1B, 5A, 6A, column 9 lines 34-67).* Leon fail to teach an inventive concept of storing information about a plurality of users using the plurality of terminals in a database remote from the plurality of securing the information about the users in the database by one or more of cryptographic devices remote from the plurality of user terminals storing a plurality of security device transaction data wherein each transaction data is related to one of the plurality of users and a cryptographic device manages value of available for the value bearing item. However Cordery et al teaches an inventive concept of storing information about a plurality of users using the plurality of terminals in a database remote from the plurality of securing the information about the users in the database by one or more of cryptographic devices remote from the plurality of user terminals storing a plurality of security device transaction data wherein each transaction data is related to one of the plurality of users (*see abstract, fig 1, 4, 5, column 4 line 23-49)* and a cryptographic device manages value of available for the value bearing item (*see figs 1, 3 and 5, column 1 lines 24-65,).* Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Leon's inventive concept to include Cordery et al's an inventive concept of storing information about a plurality of users using the plurality of terminals in a database remote from the plurality of securing the information about the users in the database by one or more of cryptographic devices remote from the plurality of user terminals storing a plurality of security device transaction data wherein each transaction data is related to one of the plurality of users and a cryptographic device manages value of available for the value bearing item because this would have protected the privacy of those transaction and the privacy of the user thereby making easier for the system to retrieve and

identify the user of the system. thereby eliminated stolen and relocated meter problems and simplifies meter management in general.

68. As per claim 105, Leon teaches a method of printing the value bearing item (*see fig 9)*.

69. As per claim 106, Leon teaches a method of loading a security device transaction data related to a user into one of the one or more of cryptographic devices when the user requests to operate on a value bearing item (*see column 9 lines 28-33, 13 lines 48-62, 15 lines 23-32)*.

70. As per claim 107, Leon teaches a method of loading a security device transaction data related to the cryptographic device when the user requests to operate on a value bearing item (*see column 9 lines 28-33, 13 lines 48-62, 15 lines 23-32)*.

71. As per claim 108, Leon teaches a method of authenticating the identity of each user and verifying that the identified user is authorized to assume a role and to perform a corresponding operation (*see column 8 lines 45-9 line 10)*.

72. As per claims 109-115, Leon teaches a method of determining an uninitialized state, an initialized state, an operational state, an administrative state, an exporting shares state, an importing shares state, and an error state (*see fib 5A, 6A, column 9 lines 45-67)*.

73. As per claims 116-120, Leon teaches a method of printing a postage value including a postal indicium comprises a digital signature, a postage amount, or a ticket (*see fig 9)*.

Response to Arguments

77. Applicant's arguments filed November 6th, 2004 have been fully considered but they are not persuasive.

a. Applicant argues the prior arts fail to teach an inventive concept of a wherein once the user is authenticated, the cryptographic device enters an operational state in which it continues to authenticate the user with respect to one or more transactions requested by the user. Cordery et al taken in combination with Leon teach an inventive concept that provide to a remote user device a cryptographic key corresponding to a postage security account at a data center; combining the password and the cryptographic key to obtain a user authentication key; performing an authentication algorithm using the user authentication key to obtain a remote access message; sending the remote access message to the data center to initiate a request for access to the postage security account by the remote user device; and authenticating the remote user device requesting access to the postage security account by verifying the remote access message. Cordery et al further teach a server that receives a request for a meter transaction from mailer. The application software in the Function Server controls the processing of the transaction request. Function Server accesses mailer database and meter database to obtain records, including the appropriate meter record, corresponding to the meter account of the mailer

initiating the request. Function Server communicates mailer records from mailer database to authentication box, which then authenticates the mailer requesting the transaction. Once the mailer has been authenticated, Function Server communicates the appropriate meter record to meter box, which verifies a signature and freshness data for the record. Meter box decrypts the encrypted key(s) that are stored within meter record, performs accounting functions on the ascending and descending registers in meter record and uses the key(s) to generate a token for the requested transaction. Meter box then generates data for an indicium, and once again signs meter record. The updated and signed record is then sent back to Database Server here it is stored as part of meter database.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The examiner can normally be reached on Mon-Thu 9:00 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on (703) 305-9768. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firmin Backer
Primary Examiner
Art Unit 3621

January 4th, 2005